UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/489,111	01/21/2000	John F. Ellingson	097823370-002	5382

7590 12/03/2003

Joseph A.Mahoney
Sonnenschein Nath & Rosenthal
8000 Sears Tower
233 South Wacker Drive
Chicago, IL 60606-6404

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/489,111	ELLINGSON, JOHN F.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on January 8, 2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and ***generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words***. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The examiner notes that the abstract is longer than 150 words and consists of 3 paragraphs and should be amended to not exceed 150 words and consist of a single paragraph.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1-2,4-6,8-17, and 20 are rejected under 35 U.S.C. 102(a) as being anticipated by Yu et al.

As per claims 1,8-10,13, and 14, it is disclosed by Yu et al of an enrollment system for verifying the identity of a user (col. 3, lines 15-27). It is comprised of non-biometric (alphanumeric input) devices and biometric (input) devices (col. 5, lines 54-56,64-66). A biometric server is connected to a (header file) database that contains the password files (alphanumeric data according to a first set of criteria) associated to a user's identity and matches (by searching) passwords (alphanumeric signals) inputted (submitted) by a user (col. 4, lines 15-28 and col. 10, lines 44-60). The biometric server (comprising a processor) compares and determines (scores) if the submitted individual's (user's) data matches (by means of a search engine) the records stored in the database by determining if the data is equivalent (acceptable or unacceptable) to a predefined statistical level of confidence (score according to a second predetermined second set of criteria)(col. 10, lines 44-60 and col. 11, lines 5-13). An authentication center (identity

escrow database) is associated with the database connected to the biometric server (comprising a processor) and compares the biometric data (exemplar) submitted from the individual users by entry into the biometric (input) devices against the stored biometric data (exemplar) submitted at enrollment (col. 5, lines 64-66, col. 8, lines 9-20). The authentication center (identity escrow database) encrypts (third predetermined set of criteria) both the password, that is associated with a user name or user id(indicative of the approved identity signal), and the biometric data to create a subfile for each user that is stored in the authentication center (identity escrow database) as enrollment information used for later comparison (col. 13, lines 20-35). The authentication center (identity escrow database) later uses live data (second input biometric data signals checked by verification means) as submitted by a user to compare it to selected records (pre-existing biometric data) of enrolled individuals whose associated identity agrees with the claimed identity and the information is then provided to a bank (third party) based upon whether there is a match (col. 4, lines 14-22, col. 8, lines 48-64, and col. 13, lines 48-55).

As per claim 2, it is recited by Yu et al that the (header file) database comprises information pertaining to bank account opening data (col. 15, lines 49-52 and col. 18, lines 1-2).

As per claim 4, Yu et al teaches of conducting banking business (e-commerce) over the Internet (col. 4, lines 30-47 and col. 15, lines 49-52).

As per claim 5, Yu et al discloses of matching a first and second biometric signal according to an appropriate standard of sensitivity for the biometric (input) device (col. 5, lines 64-66 and col. 11, lines 5-13).

As per claim 6, Yu et al discloses of storing the biometric information in an authentication center that is in a central location (central biometric authority database)(col. 18, lines 44-49).

As per claims 11,12, and 17, Yu et al discloses of an authentication center (identity escrow database) later using live data (second input biometric data signals checked by verification means) as submitted by a user to compare it to selected records (pre-existing biometric data) of enrolled individuals whose associated identity agrees with the claimed identity and the information is then provided to a bank (third party) based upon whether there is a match (col. 4, lines 14-22, col. 8, lines 48-64, and col. 13, lines 48-55).

As per claims 15 and 16, Yu et al discloses of an enrollment system for verifying the identity of a user (col. 3, lines 15-27). A biometric server is connected to a (header file) database that contains the password files (shared PINs) associated to a user's identity and matches (by searching) passwords (PIN) inputted (submitted) by a user (col. 4, lines 15-28 and col. 10, lines 44-60).

As per claim 20, it is recited by Yu et al that the biometric servers (performing enrollment and verification) run in parallel (col. 14, lines 1-7).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 3,7,18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yu et al.

As per claim 3, Yu et al discloses of a biometric server (comprising a processor) compares and determines (scores) if the submitted individual's (user's) data matches (by means of a search engine) the records stored in the database by determining if the data is equivalent (acceptable or unacceptable) to a predefined statistical level of confidence (score according to a second predetermined second set of criteria)(col. 10, lines 44-60 and col. 11, lines 5-13). The teachings of Yu et al are silent in disclosing of criteria being mathematically correlated to the per capita rate of fraud arrests in the United States. The examiner asserts that it is obvious to make use of this feature. It is obvious that criteria corresponding to fraud arrests is accounted for in order to provide assurance that a user's identity is properly established prior to allowing a user to conduct business transactions in order to avoid insurance companies paying for fraudulent purchases. Yu et al recognizes the need to avoid fraud by reciting of fraud being a growing problem on Web transactions and the need for maintaining confidentiality and integrity in transactions (col. 1, lines 60-67). It is obvious that the teachings of Yu et al provide means for mathematically correlated to the per capita rate

of fraud arrests in the United States in order to maintain confidentiality and integrity of web transactions.

As per claims 7,18, and 19, Yu et al teaches of generation of a digital certificate that is associated with a user (col. 4, lines 62-64 and col. 18, line 24-27). An authentication center (identity escrow database) later using live data (second input biometric data signals checked by verification means) as submitted by a user to compare it to selected records (pre-existing biometric data) of enrolled individuals whose associated identity agrees with the claimed identity and the information is then provided to a bank (third party) based upon whether there is a match (col. 4, lines 14-22, col. 8, lines 48-64, and col. 13, lines 48-55). Also recited by is Yu et al is conducting banking business (e-commerce) over the Internet (col. 4, lines 30-47 and col. 15, lines 49-52). Although the teachings of disclose of the use of a digital certificate associated with a user that proves trustworthiness to a potential third party member as they conduct business over the Internet, the teachings are silent in disclosing of providing warranty insurance coverage against identity theft. They examiner hereby takes official notice that the use of warranty insurance against identity theft is notoriously well known. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply protection in the case when a user's account has been compromised for a malicious intent and the user is given protection by allowing an insurance company to absorb the costs instead of a user. It is notoriously well known that credit cards used for user's purchases on the Internet are insured and if a user's credit card is stolen, the credit card provider provides a guarantee against loss

by a specified contingency, namely covering the amount of the purchased applied for illicit purposes. It is obvious that the teachings of Yu et al provide insurance warranties to protect against losses so that the user is not responsible if their credit card has been illegally obtained and used against the user's wishes.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on M-Th, 6:30a-4:00p, alt. Fr, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9586. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

CR
November 24, 2003